UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA,

- against -

MEMORANDUM AND ORDER
12-CR-166 (RRM)

TALEEK BROOKS,

Defendant.

----------X

ROSLYNN R. MAUSKOPF, United States District Judge.

Defendant Taleek Brooks moves, pursuant to Federal Rule of Criminal Procedure 12(b)(3), to suppress evidence recovered from files he maintained through the peer-to-peer file sharing network "GigaTribe," and, as "fruits" of that allegedly illegal search, other evidence subsequently recovered pursuant to search warrant from a computer and external hard-drives found at his home, and incriminating statements he made on the date of his arrest. (Doc. No. 23.) The government opposes the motion. (Doc. No. 24.) For the reasons below, this Court denies defendant's motion in its entirety.

I. FINDINGS OF FACT

The material facts are undisputed. Defendant Brooks used a "closed" peer-to-peer file-sharing program called GigaTribe under the username Tri-star. (Doc. No. 23-1.) The GigaTribe software allows a user to create a private peer-to-peer network through which selected files can be placed in specific folders on his computer, which files can be accessed by "friends" that the network creator or owner has specifically invited to join his private network. Once a "friend" request is accepted, the network owner grants the "friend" access solely to files that the network owner has designated for sharing with that friend.[1] Additionally, the GigaTribe software also allows users to communicate with each other via private chat. (*See* Doc. No. 23-3 ¶¶ 12–16.)

In or about December, 2011, Brooks, using the screen name "Tri-star,"[2] accepted a "friend" request from an undercover FBI agent (Doc. No. 23-2 ¶ 3.), and designated for sharing with the undercover certain files containing child pornography which Brooks placed in his shared folders. (Doc. No. 23-3 ¶¶ 21–22.) Although there is some indication in the record that Brooks may have accepted two "friend" requests from the same or two separate agents, one on November 21 and the second on December 24, (*see* Doc. No. 26-2; Doc. No. 23-2 ¶ 3), Brooks concedes that there was no chat or other communication between Brooks and the agent before Brooks accepted the "friend" request(s), and that the undercover agent did not view any of Brooks' files until after Brooks "friended" the agent and specifically designated files to be shared with the agent.

---

[1] In contrast, "open" peer-to-peer network programs automatically make all files in a user's shared folder accessible for browsing, searching, and downloading to all other users of the peer-to-peer network program. *See United States v. Caparotta*, __ F. Supp. 2d __, 2012 WL 3893741, at *1 (E.D.N.Y. Sept. 10, 2012) (discussing "open" peer-to-peer networks).

[2] In his Declaration in support of his Motion to Suppress (Doc. No. 23-1), Brooks admits: "In December 2011, I was a member of GigaTribe under the username Tri-star." *Id*. at ¶ 2.

The undercover agent learned through a private chat with Brooks that Brooks was "interested in black boys 10 years old and older" and proceeded to download nine image files and two video files depicting child pornography from Brooks. (Doc. No. 23-3 ¶¶ 23-24; Doc. No. 24-2.) Through the use of Tri-star's IP address, the undercover agent was able to ascertain Brooks' identity and home address. (Doc. No. 23-3 ¶¶ 25-26.) Pursuant to a search warrant, agents searched Brooks' home on January 13, 2012, seized a computer and two external hard-drives, and found additional files containing child pornography that appear to have been produced by Brooks. (Doc. No. 1 ¶¶ 4-7.) Brooks, who was present during the search, made incriminating statements concerning downloading and sharing child pornography.[3] (*Id*.) Brooks was charged with seven counts of sexual exploitation of a child in violation of 18 U.S.C. § 2251(a), one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(b), and four counts of distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2).

II. CONCLUSIONS OF LAW

Brooks argues that the search of his shared GigaTribe folders violated his Fourth Amendment rights for several reasons. First, Brooks claims that he has a reasonable expectation of privacy in his GigaTribe files requiring a warrant supported by probable cause before the undercover agent could "friend" him and remotely access Brooks' files. Second, Brooks cannot be said to have voluntarily consented to share his files because his consent was secured through deception. Finally, Brooks maintains that the agent trespassed in searching his shared folders, thereby violating the Fourth Amendment. Brooks further seeks to suppress all evidence recovered pursuant to the search warrant executed at his home, as well as the incriminating

[3] Brooks moves to suppress both the evidence obtained pursuant to the search warrant and his incriminating statements only on the ground that they constitute fruits of the alleged unlawful search of his GigaTribe files by the undercover agent.

statements made during his arrest, as fruits of the initial unlawful search of Brooks' GigaTribe files. The Court finds all of defendant's arguments to be without merit.

A. Reasonable Expectation of Privacy

"A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment must show that he had a 'legitimate expectation of privacy' in the place searched." *United States v. Hamilton*, 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)). "This inquiry involves two distinct questions: first, whether the individual had a subjective expectation of privacy; and second, whether that expectation of privacy is one that society accepts as reasonable." *Id*. (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

Brooks contends that he "maintained a reasonable expectation of privacy" in his GigaTribe files because the peer-to-peer network was open only to "friends." (Def. Br. (Doc. No. 23-5) at 12.) Even accepting that proposition as true, the Supreme Court has "consistently [ ] held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). In applying this principle to emerging internet technologies, courts have uniformly held that a user of a private or "closed" peer-to-peer network such as GigaTribe who makes available files to his "friends" does not have an objectively reasonable expectation of privacy in those files he shared. *See United States v. Soderholm*, 11-cr-3050, 2011 WL 5444053, at *7 (D. Neb. Nov. 9, 2011) (holding that the "defendant did not have an objectively reasonable expectation of privacy in the files stored on his computer once he designated those files for sharing with the 'friends' on his private network"); *United States v. Sawyer*, 786 F. Supp. 2d 1352, 1356 (N.D. Ohio 2011) (holding that the "[d]efendant did not have an objectively reasonable expectation of privacy in the information

that he shared over GigaTribe"); *United States v. Ladeau*, 09-cr-40021, 2010 WL 1427523, at *5 (D. Mass. Apr. 7, 2010) (holding that once the defendant "turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable").[4] This Court joins in so holding, and finds that once Brooks accepted the undercover agent as a "friend" and designated as shared certain files to which the undercover could gain access, Brooks had no legitimate expectation of privacy in those shared files.

Brooks attempts to distinguish the weight of authority by noting that in *Sawyer* and *Ladeau*, the government gained access to the defendant's computer by using the identity of a third-party to whom the defendant had already granted access. (Def. Br. (Doc. No. 23-5) at 12.) In those cases, each defendant had accepted "friend" requests from third parties, and the third parties provided the government with consent to use the "friend's" computer account to view the files that Sawyer and Ladeau shared with the third parties. Those courts held that once a defendant granted his "friend" access to his files, he had "no control over the manner in which his friends used that access," including turning over what they access to law enforcement. *U.S. v. Sawyer*, 786 F. Supp. 2d at 1356 (citing *Ladeau*, 2010 WL 1427523, at *1–5). Here, Brooks has even less of an objective expectation of privacy than Sawyer and Ladeau because Brooks directly "friended" the undercover agent and specifically made available to him the files in his shared folders. Indeed, if Sawyer and Ladeau assumed the risk that one of his "friends" would alert law enforcement to the fact that he was trading child pornography, Brooks equally assumes the risk that one of his "friends" is *actually* a law enforcement agent. *See Soderholm*, 2011 WL 5444053, at *7 ("The fact that the defendant's files were restricted to designated 'friends' does

[4] Likewise, courts have consistently held that users of "open" peer-to-peer networks do not have an objectively reasonable expectation of privacy in the contents of their shared folders. *See United States v. Stults*, 575 F.3d 834, 841–43 (8th Cir. 2009); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008); *United States v. Norman*, 09-CR-118-WKW, 2010 WL 3825601, at *2 (M.D. Ala. Sept. 24, 2010) *aff'd*, 448 F. App'x 895 (11th Cir. 2011).

not alter the fact that the files were no longer kept private, and the defendant bore the risk that the contraband material that he shared with his 'friends' would find its way into the possession of law enforcement officers.").

B. Consent

Even assuming *arguendo* that Brooks somehow had a protected expectation of privacy in the shared files stored on his computer, Brooks gave the undercover agent lawful, voluntary consent to remotely access those shared files, thereby rendering the warrantless search of those files reasonable. *See United States v. Garcia*, 56 F.3d 418, 422 (2d Cir. 1995); *United States v. Sanchez*, 635 F.2d 47, 59 (2d Cir. 1980). The government bears the burden of proving by a preponderance of the evidence that the consent was voluntary. *United States v. Snype*, 441 F.3d 119, 131 (2d Cir. 2006). Courts look to the totality of the circumstances to determine whether the "consent was 'a product of that individual's free and unconstrained choice, rather than a mere acquiescence in a show of authority.'" *Garcia*, 56 F.3d at 422 (quoting *United States v. Wilson*, 11 F.3d 346, 351(2d. Cir. 1993)). "So long as the police do not coerce consent, a search conducted on the basis of consent is not an unreasonable search." *Id*. (citing *Schneckloth*, 412 U.S. 218, 228 (1973)). The search must not exceed the scope of the consent given, and is measured under the standard of "objective reasonableness": that is, "what would the typical reasonable person have understood by the exchange between the officer and the suspect?" *Id*. at 423 (citing *Florida v. Jimeno*, 500 U.S. 248, 251 (1991)). As such, a search will be deemed reasonable when, "under the circumstances, it is objectively reasonable for the officer to believe that the scope of the suspect's consent permitted him to conduct the search that was undertaken." *Id*. (citing *Jimeno*, 500 U.S. at 249 (internal brackets and quotations omitted)).

It is undisputed here that Brooks made available to the undercover agent files containing child pornography that could be found in Brooks' shared GigaTribe folders, and that Brooks intended to deliberately share those files with the undercover agent by accepting the undercover agent's "friend" request and placing the files to which he has granted access into his shared folders. Indeed, the express purpose of GigaTribe itself, and in designating shared folders, is to allow "friends" specifically selected by the GigaTribe network owner to browse and download files contained in those shared folders. Furthermore, as the record clearly indicates, and Brooks does not dispute, the undercover agent did not exceed the scope of Brooks' consent. The undercover agent only browsed the files contained within the folders designated by Brooks for sharing, and it was solely within these folders that the undercover agent observed the files that he had probable cause to believe contained child pornography. Consequently, this Court finds that Brooks gave the undercover agent consent to search his shared GigaTribe folders and that this search does not implicate Brooks' Fourth Amendment rights.

The fact that that the undercover agent did not identify himself as law enforcement and may have deceived Brooks as to his true identity does not render the consent involuntary or invalid. *See Sawyer*, 786 F. Supp. 2d at 1356 ("Simply because the government obtained access to these files through the use of a ruse does not render the consent involuntary.") "[I]t has long been acknowledged by the decisions of this Court . . . that, in the detection of many types of crime, the Government is entitled to use decoys and to conceal the identity of its agents." *Lewis v. U.S.*, 385 U.S. 206, 208–09 (1966) (citations omitted). This is not "the kind of 'extreme' misrepresentation of investigatory purpose by which a person is 'deprived[d] . . . of the ability to make a 'fair assessment of the need to surrender his privacy' . . . [but rather] 'the deception in question was the use of an undercover agent who obtained otherwise voluntary consent through

the use of his adopted identity." *United States v. Pollaro*, 733 F. Supp. 2d 364, 369 (E.D.N.Y. 2010) (citing *United States v. Montes–Reyes*, 547 F. Supp. 2d 281, 287–91 (S.D.N.Y.2008)). Indeed, to accept defendant's argument would completely eviscerate the government's ability to conduct undercover operations in which its agents adopt fictitious identities.

Nor is this the type of search found unreasonable in *United States v. Gouled*, 255 U.S. 298 (1921), *overruled on other grounds*, *Warden v. Hayden*, 387 U.S. 294 (1967), on which defendant heavily relies. In *Gouled*, an acquaintance of the defendant, at the direction of law enforcement, gained entrance to the defendant's home under the guise of making a social call, and thereafter, surreptitiously entered the defendant's office, searched it, and seized documents. The Court found the search and seizure to be unreasonable, emphasizing that the initial entry under the circumstances presented, obtained by stealth, was tantamount to the government's use of force or coercion:

> The prohibition of the Fourth Amendment is against all unreasonable searches and seizures and if for a Government officer to obtain entrance to a man's house or office by force or by an illegal threat or show of force, amounting to coercion, and then to search for and seize his private papers would be an unreasonable and therefore a prohibited search and seizure, as it certainly would be, it is impossible to successfully contend that a like search and seizure would be a reasonable one if only admission were obtained by stealth instead of by force or coercion. The security and privacy of the home or office and of the papers of the owner would be as much invaded and the search and seizure would be as much against his will in the one case as in the other, and it must therefore be regarded as equally in violation of his constitutional rights.

Gouled, 255 U.S. at 305-06. In contrast, here, without any prompting,[5] Brooks invited his "friend" to remotely access the files Brooks had specifically placed into his shared folders, and the undercover agent did no more than that which Brooks invited him to do. Indeed, "a government agent, in the same manner as a private person, may accept an invitation to do

[5] The record indicates that no conversation took place until after Brooks accepted the undercover agent's "friend" request and was consequently allowed to search Brooks' shared GigaTribe folders.

business and may enter another's premises for the very purposes contemplated by the occupant." *Lewis*, 385 U.S. at 211. That is precisely what happened here. As in *Lewis*, Brooks invited the undercover agent "in," and "the agent [did not] see, hear, or take anything that was not contemplated, and in fact intended, by [the defendant] as a necessary part of his illegal business." *Id*. at 210. As such, the undercover agent's access to the files in Brooks' shared folders was reasonable under the Fourth Amendment.

C. United States v. Jones

Brooks' attempt to rely on the Supreme Court's recent decision in *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945 (2012) is misplaced.

In *Jones*, the Supreme Court found that where the "Government physically occupie[s] private property for the purpose of obtaining information . . . such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." 132 S. Ct. at 949. The Court noted that not all "technical trespass that led to the gathering of evidence" was protected by the Fourth Amendment; rather, the "Fourth Amendment protects against trespassory searches only with regard to those items ('persons, houses, papers, and effects') that it enumerates." *Id*. at 953, n.8. Moreover, the Court was careful to limit its holding to physical trespass, noting that "the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test" and holding that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis." *Id*. at 952–53.

In contrast to *Jones*, there is no evidence here that the undercover agent made any physical intrusion on a constitutionally protected area. The agent did not install any device or software on Brooks' computer to enable monitoring or tracking, did not physically enter Brooks'

home, and did not physically access his computer. *See id*. at 950 (noting that "wiretaps attached to telephone wires on the public streets did not constitute a Fourth Amendment search because '[t]here was no entry of the houses or offices of the defendants' (citing *Olmstead v. United States*, 277 U.S. 438, 464 (1928)). Nor did the agent remotely access any of Brooks' computer files until after Brooks granted him access, and only then did the agent access those specific files which Brooks' had designated for the agent to see. As such, the undercover agent did not physically intrude on any of Brooks' constitutionally protected areas. Therefore, because this situation involves "merely the transmission of electronic signals without trespass," the *Katz* reasonable-expectation-of-privacy governs this analysis, which, as discussed above, does not implicate Brooks' Fourth Amendment rights. Indeed, at least one court has rejected the very argument Brooks attempts to advance here. *See United States v. Nolan*, 11-cr-82, 2012 WL 1192183, at *10–11, (Report and Recommendation), adopted by 2012 WL 1192757, at *1 (E.D. Mo. Apr. 9, 2012) (rejecting the defendant's argument that under *Jones* an undercover agent was required to obtain a warrant before searching his shared folder on a peer-to-peer network because "[t]here is no evidence that the police installed any device or software on the defendant's computer that enabled them to monitor or track his usage").

D. Fruit of the Poisonous Tree

Since the initial search of Brooks' shared GigaTribe folders does not implicate the Fourth Amendment, there is no 'poisonous tree' and therefore there can be no 'poisonous fruit' warranting suppression. *See United States v. Antonelli*, 434 F.2d 335, 338 (2d Cir. 1970). Thus, both the evidence obtained pursuant to the search warrant of Brooks' home, as well as Brooks' incriminating statements, cannot be the product of a Fourth Amendment violation as defendant claims. Brooks does not raise any other challenges to this evidence. For example, he does not

challenge the sufficiency of the search warrant itself or its manner of execution, nor does he challenge the adequacy of the *Miranda* warnings, his waiver thereof, or the voluntariness of his statements. Thus, on the Fourth Amendment grounds on which it is based, Brooks' motion to suppress fails.

CONCLUSION

For the reasons set forth herein, defendant Brooks' motion to suppress is DENIED.

SO ORDERED.

Dated: Brooklyn, New York
December 17, 2012

Roslynn R. Mauskopf

ROSLYNN R. MAUSKOPF
United States District Judge